

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/EP05/051072

International filing date: 10 March 2005 (10.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: DE
Number: 10 2004 014 435.4
Filing date: 24 March 2004 (24.03.2004)

Date of receipt at the International Bureau: 03 June 2005 (03.06.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PATENT COOPERATION TREATY

From the RECEIVING OFFICE

PCT

To:

The International Bureau of WIPO
34, chemin des Colombettes
1211, Geneva 20
Suisse

The International Searching Authority

NOTIFICATION CONCERNING
DOCUMENTS TRANSMITTED

Date of mailing
(day/month/year)

03.06.2005

International application No.

PCT/EP2005/051072

The receiving Office transmits herewith the following documents:

1. the record copy (Article 12(1)) (only for the IB).
2. the search copy of form PCT/RO/101 (Article 12(1)) (only for the ISA).
3. the confirmation copy (Administrative Instructions, Section 331) (only for the IB).
4. substitute sheets (Administrative Instructions, Section 325(a)).
5. later submitted sheets (Administrative Instructions, Section 309(b)(iii), (c)(ii)).
6. later submitted drawings (Administrative Instructions, Section 310(c)(iii), (d)(ii)).
7. other document(s):

letter(s) dated: 29-04-2005

power(s) of attorney (only for the IB).

statement(s) explaining lack of signature considered to be satisfactory by this receiving Office (only for the IB).

priority document(s) (only for the IB).

fee calculation sheet (only for the IB).

document(s) concerning deposited biological material.

nucleotide and/or amino acid sequence listing(s) in computer readable form (only for the ISA).

PCT EASY diskette (only for the IB).

earlier search(es) (only for the ISA).

Form PCT/RO/106.

Form PCT/RO/

Name and mailing address of the Receiving Office

European Patent Office, P.O. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel. (+31-70) 340-2040
Fax: (+31-70) 340-3016

Authorized officer

J.C. de BRUIJN

SIEMENS

EPO - Munich
59

04. Mai 2005

Cd

Europäisches Patentamt
80298 München

Name: Karola Theiss
Abteilung: CT IP S AM
Standort: Frankfurt / Main
Telefon: +49 694 0805 369
Fax: +49 694 0805 370
E-Mail: karola.theiss@siemens.com

Ihr Schreiben
Unser Zeichen: 2004P03719WO
Datum: 29. April 2005

Anmeldung Nr. PCT/EP2005/051072
Anmelder Siemens Aktiengesellschaft

Zur obengenannten Anmeldung werden die nachfolgend genannten Unterlagen nachgereicht:

Prioritätsbeleg(e) 10 2004 014 435.4 ✓

Siemens Aktiengesellschaft

i.v. Richter

Dr. Richter
Allg. Vollmacht Nr. 650

IDNR: 4068 / V: 99-1.00 / B:Val

Corporate Technology

Corporate Intellectual Property and Functions

Leitung:
Dr. Winfried Büttner

Zustelladresse:
Siemens AG

Postfach 22 16 34
80506 München

Hausadresse:
Kruppstr. 105
60388 Frankfurt

Siemens Aktiengesellschaft · Vorsitzender des Aufsichtsrats: Heinrich v. Pierer · Vorstand: Klaus Kleinfeld, Vorsitzender;
Johannes Feldmayer, Thomas Ganswindt, Edward G. Krubasik, Rudi Lamprecht, Heinz-Joachim Neubörger, Jürgen Radomski,
Erich R. Reinhardt, Ulf J. Sharef, Claus Weyrich, Klaus Wucherer
Sitz der Gesellschaft: Berlin und München · Registergericht: Berlin-Charlottenburg, HRB 12300; München, HRB 6684

Ausgehend von den Problemen und Nachteilen des Standes der Technik liegt der Erfindung die Aufgabe zugrunde, eine Anordnung der eingangs genannten Art zu schaffen, welche höchsten Anforderungen der Manipulationssicherheit genügt und gleichzeitig eine Eignung für die Serienproduktion bei geringeren Kosten aufweist.

Die erfindungsgemäße Aufgabe wird mittels eines integrierten Schaltkreises der eingangs genannten Art gelöst, welcher eine Verschlüsselungseinheit als Funktionsmodul umfasst, mittels 10 derer Daten oder Programmcode verschlüsselbar und entschlüsselbar sind.

Dadurch, dass eine Verschlüsselungseinheit als Funktionsmodul 15 des integrierten Schaltkreises Element dieses Bauteiles ist, kann in der Fertigung und Entwicklung einer Anordnung mit einem erfindungsgemäßen integrierten Schaltkreis die zusätzliche Bereitstellung, Montage und Abstimmung auf umliegende Bauelemente eingespart werden. In synergetischer Weise ergibt 20 sich der weitere große Vorteil, dass die Verschlüsselungseinheit von dem integrierten Schaltkreis, dessen Bestandteil sie ist, nur schwer zu trennen ist und daher Versuche der Manipulation zum Scheitern verurteilt sind.

25 Die Manipulation eines erfindungsgemäßen integrierten Schaltkreises, insbesondere die Abtrennung einzelner Funktionsmodule, gestaltet sich besonders schwierig, wenn der integrierte Schaltkreis als Halbleiterchip ausgebildet ist, insbesondere, wenn einzelne Funktionsmodule puzzleartig ineinander greifen, 30 in einer Weise, dass einzelne Funktionsmodule diskret nicht mehr erkennbar sind. Hier können besonders komplexe geometrische Verstrickungen gewählt werden, so dass die miteinander vermischten Halbleiterstrukturen sich mittels einer Analyse

in Manipulationsabsicht nicht mehr als solche trennbar erkennen lassen.

Zusätzliche Sicherheit gegen Manipulation wird gewonnen, wenn
5 die Funktionsmodule einen ersten Speicher umfassen, in welchem kryptologische Schlüssel abgespeichert sind. Die Integration eines solchen ersten Speichers erschwert einen gezielten Zugriff und ein gezieltes Auslesen der kryptologischen Schlüssel.

10 Der Aufwand für eine Verwaltung kryptologischer Schlüssel durch den Hersteller der Geräte entfällt vollständig bei zusätzlichem Sicherheitsgewinn, wenn die Funktionsmodule einen Zufallszahlengenerator (RNG) umfassen, der die kryptologischen Schlüssel gleichsam autonom erzeugt. Diese Schlüssel
15 können zweckmäßig in dem ersten Speicher abgelegt werden.

Mit Vorteil kann als weiteres Funktionsmodul eine Real-Time-Clock in den integrierten Schaltkreis eingegliedert werden,
20 deren korrekte Funktion ebenfalls hohe Relevanz für die Sicherheit gegen Manipulation hat.

25 Damit der Manipulationsangriff nicht nur erschwert, sondern unmöglich gemacht wird, kann mit Vorteil eine Sicherheitssensorik in dem Schaltkreis als Funktionsmodul integriert werden, mittels derer mindestens ein Betriebsparameter des integrierten Schaltkreises überwachbar ist. Geeignete Betriebsparameter für die Überwachung sind beispielsweise die Taktfrequenz der Real-Time-Clock, der System- bzw. CPU-Takt, oder
30 eine Betriebstemperatur, oder eine Betriebsspannung des integrierten Schaltkreises, oder der Zustand einer Schutzschicht auf dem integrierten Schaltkreis, oder eine Kombination der vorgenannten Betriebsparameter. Ist der integrierte

Schaltkreis als Halbleiterbauelement ausgebildet, so ist die Überwachung des Zustandes einer Schutzschicht auf dem integrierten Schaltkreis besonders effektiv, da die Schutzschicht zerstört werden muss, um mechanisch auf der Struktur des

5 Halbleiterchips zuzugreifen. Hierbei ist es zweckmäßig, wenn die Schutzschicht als aktive Schutzschicht ausgebildet und direkt auf dem Die des Halbleiterchips aufgebracht ist. Eine zweckmäßige Weiterbildung sieht vor, dass die aktive Schutzschicht aus mindestens einer länglichen elektrischen Leitung besteht, welche entlang der Oberfläche des Dies, insbesondere

10 abschnittsweise in untereinander parallelen Bahnen verläuft. Die Überwachung kann beispielsweise eine Überwachung des ohmschen Widerstands der elektrischen Leitung sein, wobei zweckmäßig eine Änderung des Widerstandswertes, die auf eine Zerstörung der elektrischen Leitung schließen lässt, eine Löschung der zu schützenden Daten bewirkt. Vorzugsweise wird der Mikrocontroller in einen gesicherten Zustand, beispielsweise Reset, überführt. Auf diese Weise wird das System "integrierter Schaltkreis" nach der Erfindung vergleichsweise

15 20 eigensicher.

Zweckmäßig gestaltet sich die Überwachung des Betriebsparameters in der Weise, dass mindestens ein Grenzwert für den zu überwachenden Betriebsparameter vorgegeben ist, der Betriebsparameter gemessen und mit dem Grenzwert verglichen wird und bei einem Überschreiten oder Unterschreiten des Grenzwertes der Inhalt des ersten Speichers gelöscht wird. Zweckmäßig ist der Grenzwert so zu wählen, dass die Vorgaben des Normalbetriebs nicht zu einer Funktionsunterbrechung der Anordnung führen, beispielsweise im Automotive-Bereich bei einer Temperatur von -40 °C noch keine Löschung der Daten erfolgt.

Die Handhabbarkeit und Sicherheit des erfindungsgemäßen integrierten Schaltkreises erhöht sich zusätzlich, wenn er in einem Gehäuse angeordnet ist und aus dem Gehäuse herausgeföhrte Anschlusskontakte aufweist. Zum Zweck einer mechanischen Manipulation müsste demgemäß zunächst das Gehäuse geöffnet werden.

Eine höhere Integration des erfindungsgemäßen Schaltkreises kann erreicht werden, wenn einzelne Funktionsmodule eine im Wesentlichen flächige Erstreckung aufweisen und in Richtung der Flächennormalen benachbart zueinander angeordnet sind. So kann zum Beispiel die zentrale Verarbeitungseinheit gestapelt mit verschiedenen Speichern oder anderen Funktionsmodulen angeordnet werden.

Mit Vorteil können Angriffe, die Rückschlüsse auf den Funktionszustand aus dem Verhalten des Versorgungsstromes des integrierten Schaltkreises schließen, abgewehrt werden, wenn die Funktionsmodule einen integrierten Spannungsregler umfassen, der die Betriebsspannung regelt und auf diese Weise nach außen hin diesen Betriebsparameter vergleichsweise vertrauscht.

Besondere Vorteile entfaltet der erfindungsgemäße integrierte Schaltkreis in einer Anordnung mit einem zweiten Speicher, der mittels eines Datenbusses mit dem erfindungsgemäßen integrierten Schaltkreis in Verbindung steht, in welchem zweiten Speicher Daten oder Programmcode verschlüsselt abgelegt sind und der Speicherzellen aufweist, welche jeweils eine Speicheradresse aufweisen und jede Speicherzelle direkt lesend oder schreibend angesprochen werden kann. Um die gesamte Anordnung gegenüber dem Ausfall einer externen Spannungsversorgung abzusichern, ist es zweckmäßig, wenn sie mit einer

Batterie in Verbindung steht, so dass die Spannungsversorgung bei einem Fehlen anderer Energieversorgung aufrechterhaltend ist. Insofern lassen sich auch Kosten einsparen, wenn der zweite Speicher kostengünstig flüchtig ausgebildet und mittels der Batterie abgepuffert ist.

Ersatzweise oder in Ergänzung zu dem zweiten Speicher kann ein dritter Speicher zweckmäßig sein, der mit dem integrierten Schaltkreis mittels eines Datenbusses in Verbindung steht und nicht flüchtig ausgebildet ist, insbesondere als Flash oder ROM ausgebildet ist, wobei in dem dritten Speicher die Daten oder Programmcode vorzugsweise verschlüsselt abgelegt sind.

Besonders vorteilhaft ist eine Abpufferung der Sicherheitssensorik mittels einer Batterie. Alternativ oder in Ergänzung zu dieser Maßnahme kann eine in dem Gehäuse integrierte Hilfsenergiequelle, beispielsweise ein Kondensator, vorgenommen sein, welcher die Energie im Falle eines registrierten Manipulationsversuches zum Löschen der Speicher, insbesondere des ersten Speichers, bereitstellt.

Im Folgenden ist die Erfindung anhand eines speziellen Ausführungsbeispiels zur Verdeutlichung näher beschrieben. Neben diesem Ausführungsbeispiel ergeben sich für den Fachmann aus der hier beschriebenen Erfindung zahlreiche andere Möglichkeiten der Gestaltung. Insbesondere sind der Erfindung auch Merkmalskombinationen zuzurechnen, welche sich aus Kombinationen der Ansprüche ergeben, auch wenn kein ausdrücklicher dementsprechender Rückbezug angeführt ist. Es zeigen:

Figur 1 eine schematische Darstellung einer erfindungsgemäßen Anordnung.

Figur 1 zeigt einen integrierten Schaltkreis 1 mit verschiedenen Funktionsmodulen 2, der mit externen Bauelementen 3 in Verbindung steht. Der integrierte Schaltkreis weist neben einer zentralen Verarbeitungseinheit 4 noch weitere Funktionsmodule 2 auf, nämlich einen Cachespeicher 5, eine Verschlüsselungseinheit 6, einen ersten Speicher 7, eine Real-Time-Clock 8, einen Zufallszahlengenerator 80 und eine Sicherheitssensorik 9. Daneben sind ein Spannungsregler 10 und eine Hilfsenergiequelle 12 integrierte Bauelemente des als Halbleiterchip 13 ausgebildeten integrierten Schaltkreises 1. Die zentrale Verarbeitungseinheit 4 verarbeitet Daten oder führt Programme aus, welche sie mittels eines ersten Datenbusses 15 aus dem Cachespeicher 5 ausliest.

Der Cachespeicher 5 steht mit der Verschlüsselungseinheit 6 mittels eines zweiten Datenbusses 16 in Verbindung. Die Verschlüsselungseinheit 6 liest aus dem zweiten oder dritten Speicher 40, 41 mittels des Adress-Datenbusses 32 die verschlüsselten Daten bzw. Code ein, entschlüsselt sie mittels des im ersten Speicher 7 abgelegten kryptografischen Schlüssels 18 und schreibt sie in den Cache bzw. in andere interne Register der zentralen Verarbeitungseinheit 4. Die kryptologischen Schlüssel 18 sind zuvor von dem Zufallszahlengenerator 80 erzeugt worden. Der Zufallszahlengenerator 80 verwendet zur Erzeugung der kryptografischen Schlüssel 18, welche im ersten Speicher 7 abgelegt sind beispielsweise die Startwerte aus den statistischen Schwankungen (Rauschen) von internen, physikalischen Messgrößen, wie Chiptemperatur, Versorgungsspannung, Taktfrequenz.

30

Die Sicherheitssensorik 9 überwacht neben der Betriebstemperatur T , der Betriebsspannung U , der Taktfrequenz f auch den ohmschen Widerstand R einer Schutzschicht 20, welche aus zu-

einander im Wesentlichen parallelen Bahnen einer elektrischen Leitung 21 besteht, die direkt auf dem Die des Halbleiterchips 13 aufgebracht sind. Der gemessene Widerstand R wird permanent mit einem Grenzwert verglichen, und bei Überschreitung des Grenzwertes veranlasst die zentrale Verarbeitungseinheit 4 die Löschung des ersten Speichers 7, wobei der integrierte Schaltkreis 1 anschließend in einen gesicherten Zustand, beispielsweise Reset, überführt wird.

Der integrierte Schaltkreis 1 ist von einem Gehäuse 30 umgeben, welches Anschlusskontakte 31 aufweist, die zumindest teilweise mit einem Adress-Datenbus 32 in Verbindung stehen. Mittels des Adress-Datenbusses 32 tauscht der integrierte Schaltkreis 1 Daten mit einem zweiten Speicher 40 und einem dritten Speicher 41 aus. Der zweite Speicher 40 ist als flüchtiges RAM ausgebildet und mittels einer Batterie 43 gegen Spannungsausfall ebenso wie der integrierte Schaltkreis 1 abgesichert. Der dritte Speicher 41 ist nicht flüchtig als Flash oder ROM ausgebildet. Die in dem zweiten Speicher 40 und dritten Speicher 41 abgelegten Daten sind unter Verwendung der kryptologischen Schlüssel 18 verschlüsselt und werden bei jedem Zugriff mittels der Verschlüsselungseinheit 6 verschlüsselt oder entschlüsselt.

Patentansprüche

1. Integrierter Schaltkreis (1) mit Funktionsmodulen (2), wobei die Funktionsmodule (2) eine zentrale Verarbeitungseinheit (4), mittels welcher Daten verarbeitbar und Programme ausführbar sind, und einen Cachespeicher (5) umfassen, dadurch gekennzeichnet, dass die Funktionsmodule (2) eine Verschlüsselungseinheit (6) umfassen, mittels welcher Daten verschlüsselbar und entschlüsselbar sind.
2. Integrierter Schaltkreis (1) nach Anspruch 1, dadurch gekennzeichnet, dass die Funktionsmodule einen Zufallszahlengenerator (80) umfassen.
3. Integrierter Schaltkreis (1) nach Anspruch 1, dadurch gekennzeichnet, dass die Funktionsmodule (2) einen ersten Speicher (7) umfassen, in welchem kryptologische Schlüssel (18) abgespeichert sind.
4. Integrierter Schaltkreis (1) nach Anspruch 2 und 3, dadurch gekennzeichnet, dass kryptologische Schlüssel (18), welche in dem ersten Speicher (7) abgespeichert sind, mittels des Zufallszahlengenerators (80) erzeugt sind.
5. Integrierter Schaltkreis (1) nach Anspruch 1, dadurch gekennzeichnet, dass die Funktionsmodule (2) eine Real-Time-Clock (8) umfassen.
6. Integrierter Schaltkreis (1) nach Anspruch 1, dadurch gekennzeichnet, dass die Funkti-

onsmodule (2) eine Sicherheitssensorik (9), mittels derer mindestens ein Betriebsparameter (f, T, U) des integrierten Schaltkreises (1) überwachbar ist, umfassen.

7. Integrierter Schaltkreis (1) nach Anspruch 6, durch gekennzeichnet, dass der Betriebsparameter (f, T, U) die Taktfrequenz (f) der Real-Time-Clock (8) und/oder eine Betriebstemperatur (T) an einer Stelle des Integrierten Schaltkreises (1) und/oder eine Betriebsspannung (U) des integrierten Schaltkreises (1) und/oder der Zustand einer Schutzschicht (20) auf dem Integrierten Schaltkreis (1) ist.
8. Integrierter Schaltkreis (1) nach Anspruch 6, durch gekennzeichnet, dass für den zu überwachenden Betriebsparameter (f, T, U) mindestens ein Grenzwert vorgegeben ist, der Betriebsparameter (f, T, U) gemessen wird und mit dem Grenzwert verglichen wird und bei einem Überschreiten oder Unterschreiten des Grenzwertes der Inhalt des ersten Speichers gelöscht wird.
9. Integrierter Schaltkreis (1) nach Anspruch 1, durch gekennzeichnet, dass er in einem Gehäuse (30) angeordnet ist und aus dem Gehäuse (30) herausgeführte Anschlusskontakte (31) aufweist.
10. Integrierter Schaltkreis (1) nach Anspruch 1, durch gekennzeichnet, dass einzelne Funktionsmodule (2) eine im Wesentlichen flächige Erstreckung aufweisen und in Richtung der Flächennormalen benachbart zueinander angeordnet sind.

11. Integrierter Schaltkreis (1) nach Anspruch 1, durch gekennzeichnet, dass die Funktionsmodule (2) einen integrierten Spannungsregler umfassen, welcher eine Betriebsspannung (U) regelt.
- 5 12. Integrierter Schaltkreis (1) nach Anspruch 1, durch gekennzeichnet, dass er als Halbleiterchip (13) ausgebildet ist.
13. Integrierter Schaltkreis (1) nach Anspruch 12, durch gekennzeichnet, dass Halbleiterstrukturen der einzelnen Funktionsmodule (2) puzzleartig ineinander greifen, zur Vermeidung, dass einzelne Funktionsmodule (2) erkennbar sind.
14. Integrierter Schaltkreis (1) nach Anspruch 12, durch gekennzeichnet, dass direkt auf dem Die des Halbleiterchips (13) eine aktive Schutzschicht (20) aufgebracht ist, welche aus mindestens einer länglichen elektrischen Leitung (21) besteht, welche entlang der Oberfläche des Dies, insbesondere abschnittsweise in zueinander parallelen Bahnen verläuft.
- 15 20 15. Anordnung mit einem integrierten Schaltkreis (1) nach einem der Ansprüche 1 bis 14, dadurch gekennzeichnet, dass der integrierte Schaltkreis (1) mittels eines Datenbusses (32) mit einem zweiten Speicher (40) [RAM] in Verbindung steht, in welchem Daten verschlüsselt abgelegt sind, wobei der zweite Speicher (40) Speicherzellen aufweist, welche jeweils eine Speicheradresse aufweisen und jede Speicherzelle direkt lesend oder schreibend angesprochen werden kann.

16. Anordnung mit einem integrierten Schaltkreis (1) nach einem der Ansprüche 1 bis 14, dadurch gekennzeichnet, dass der zweite Speicher (40) flüchtig ist und mit einer Batterie (43) in Verbindung steht, so dass die Spannungsversorgung bei einem Fehlen anderer Energieversorgung aufrechterhalten ist.
5
17. Anordnung mit einem integrierten Schaltkreis (1) nach einem der Ansprüche 1 bis 14, dadurch gekennzeichnet, dass der integrierte Schaltkreis (1) mittels eines Datenbusses (32) mit einem nichtflüchtigen dritten Speicher (41), insbesondere einem Flash oder ROM in Verbindung steht, in welchem Daten oder Programmcode verschlüsselt abgelegt sind.
10
18. Anordnung mit einem integrierten Schaltkreis (1) nach Anspruch 6, dadurch gekennzeichnet, dass die Sicherheitssensorik (9) mit einer Batterie (43) in Verbindung steht, so dass die Spannungsversorgung bei einem Fehlen anderer Energieversorgung aufrechterhalten ist.
15
19. Anordnung mit einem integrierten Schaltkreis (1) nach Anspruch 6, dadurch gekennzeichnet, dass die Sicherheitssensorik (9) mit einer in dem Gehäuse (30) integrierten Hilfsenergiequelle (12) in Verbindung steht, welche die Energie zum Löschen ersten Speichers (7) bereitstellt.
25

Zusammenfassung

Anordnung mit einem integrierten Schaltkreis

5 Die Erfindung betrifft einen Integrierten Schaltkreis (1) mit Funktionsmodulen (2), wobei die Funktionsmodule (2) eine zentrale Verarbeitungseinheit (4), mittels welcher Daten verarbeitbar und Programme ausführbar sind, und einen Cachespeicher (5) umfassen. Die Gewährleistung einer Manipulationssicherheit derartiger Module ist bislang sehr aufwendig und geht mit hohen Kosten einher. Hier schafft die Erfindung Abhilfe, indem die Funktionsmodule (2) eine Verschlüsselungseinheit (6) umfassen, mittels welcher Daten verschlüsselbar und entschlüsselbar sind.

15

Figur 1

Bezugszeichenliste

- 1 Integrierter Schaltkreis
- 2 Funktionsmodul
- 3 Externe Bauelemente
- 4 zentrale
 Verarbeitungseinheit
- 5 Cachespeicher
- 6 Verschlüsselungseinheit
- 7 ersten Speicher
- 8 Real-Time-Clock
- 9 Sicherheitssensorik
- 10 Spannungsregler
- 12 Hilfsenergiequelle
- 13 Halbleiterchip
- 15 erster Datenbus
- 16 zweiter Datenbus
- 17 dritter Datenbus
- 18 kryptologische Schlüssel
- 20 Schutzschicht
- 21 Elektrische Leitung
- 30 Gehäuse
- 31 Anschlusskontakte
- 32 Adress-Datenbus
- 40 zweiter Speicher
- 41 dritter Speicher
- 43 Batterie
- 80 Zufallszahlengenerator
- f Taktfrequenz
- R Widerstand
- T Betriebstemperatur
- U Betriebsspannung

Fig 7

